Technical Note: How to sign a CA certificate on Windows server 2008 and import certificate for SSL inspection to a FortiGate.

Description >> This article describes about how to Sign a CA certificate on Windows server 2008 and import the certificate for SSL inspection.

Purpose of configuring SSL inspection on FortiGate unit with CA certificate signed by Windows CA: When SSL inspection for HTTPS traffic (Deepscan) is enabled on FortiGate unit, browser will display invalid certificate error while accessing HTTPS websites.

- **When SSL inspection option enabled on FortiGate unit, FortiGate unit will act as man in the middle to scan the SSL sessions. FortiGate unit will decrypt the SSL sessions and re encrypt them with its own certificate (FortiGate_CA_SSLProxy).**
- **The client browser show an error message "invalid certificate" becuase the client browser cannot validate the certificate used to encrypt the session.**
- **To overcome this behaviour, you can import the FortiGate_CA_SSLProxy certificate to client browser. But this may not be possible in large networks.**
- **In Windows Active directory Domain environments, we can generate a CA certificate signed by the Windows CA and configure the certificate for SSL inspection.**
- **Since the certificate is signed by the domain controller CA, This certificate will be trusted by all workstations which are member of the domain. Manually importing the certificates on to computers is not necessary.**

Note:-

- Mozilla Firefox and other open source browsers do not depend on the local certificate store of windows. You need to import the certificate manually in these browsers.

Expectations and Requirements;

To sign certificate using Windows CA, CA server should be installed on Windows AD.

Configuration steps

1) Generate a CSR on FortiGate unit.

2) Sign the CSR on Windows CA and download the signed certificate from Windows CA.

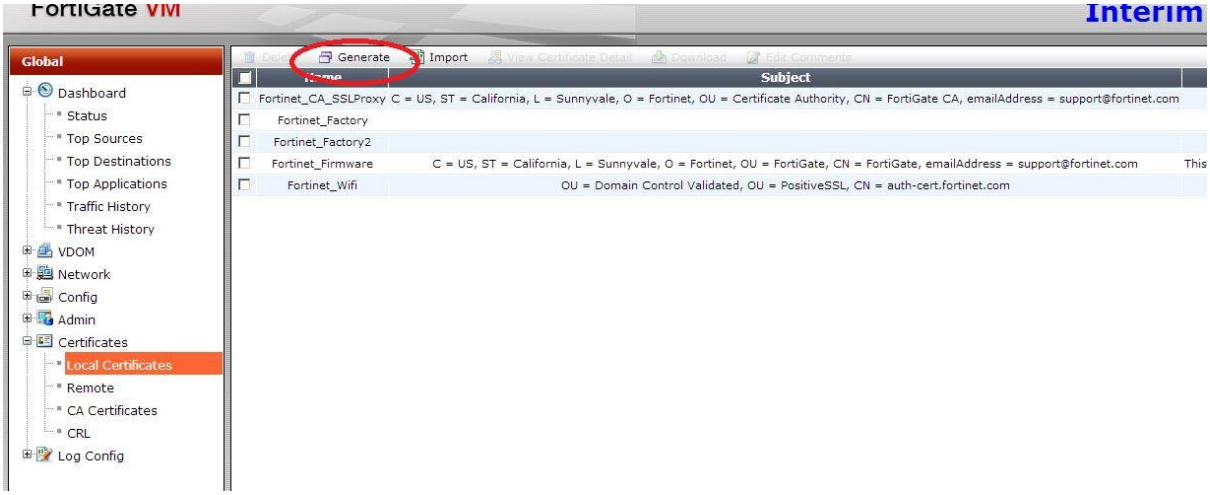
3) Import the signed certificate on to FortiGate unit.

4) Configure SSL inspection to use the new certificate.

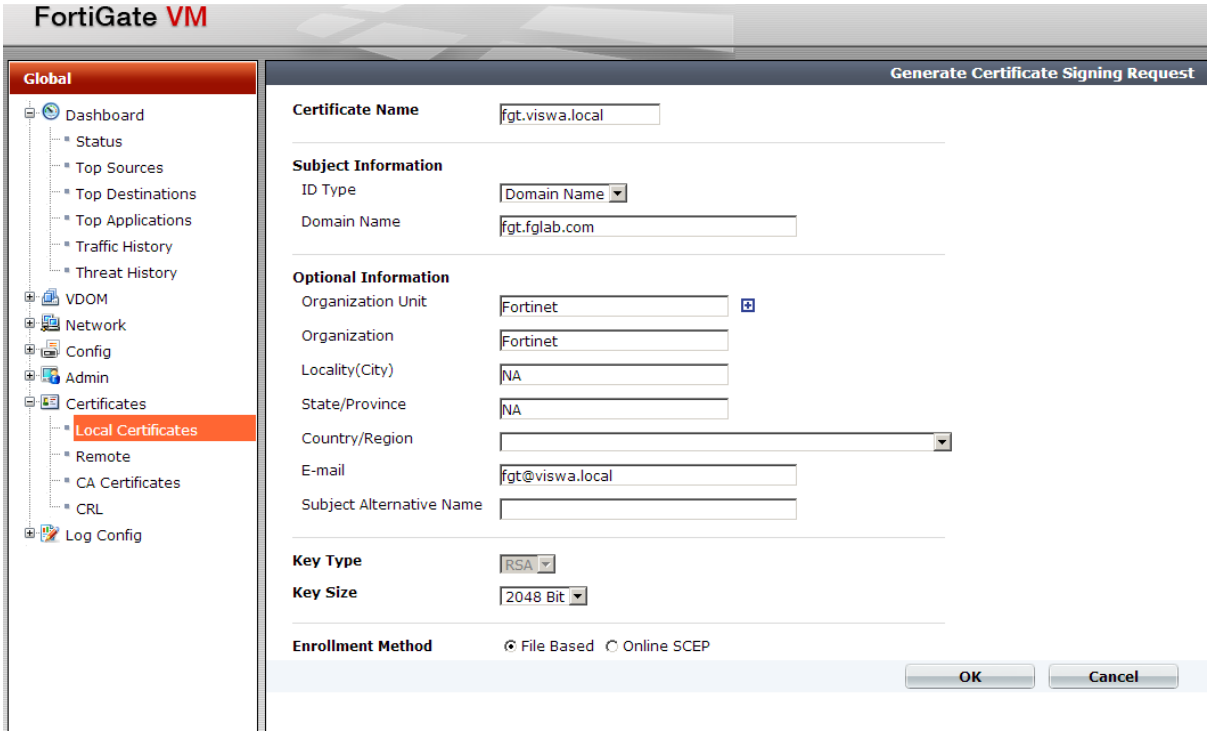
Step1

➢ Generate a Certificate Signing Request on FortiGate unit.

- Log in to FortiGate unit GUI >> Go to System >> Certificates >> Local Certificates >> Select “Generate”



- Enter the parameters as per your requirement, Select “Enrollment Method” as “File Based” and Click on OK to generate the certificate Signing request.

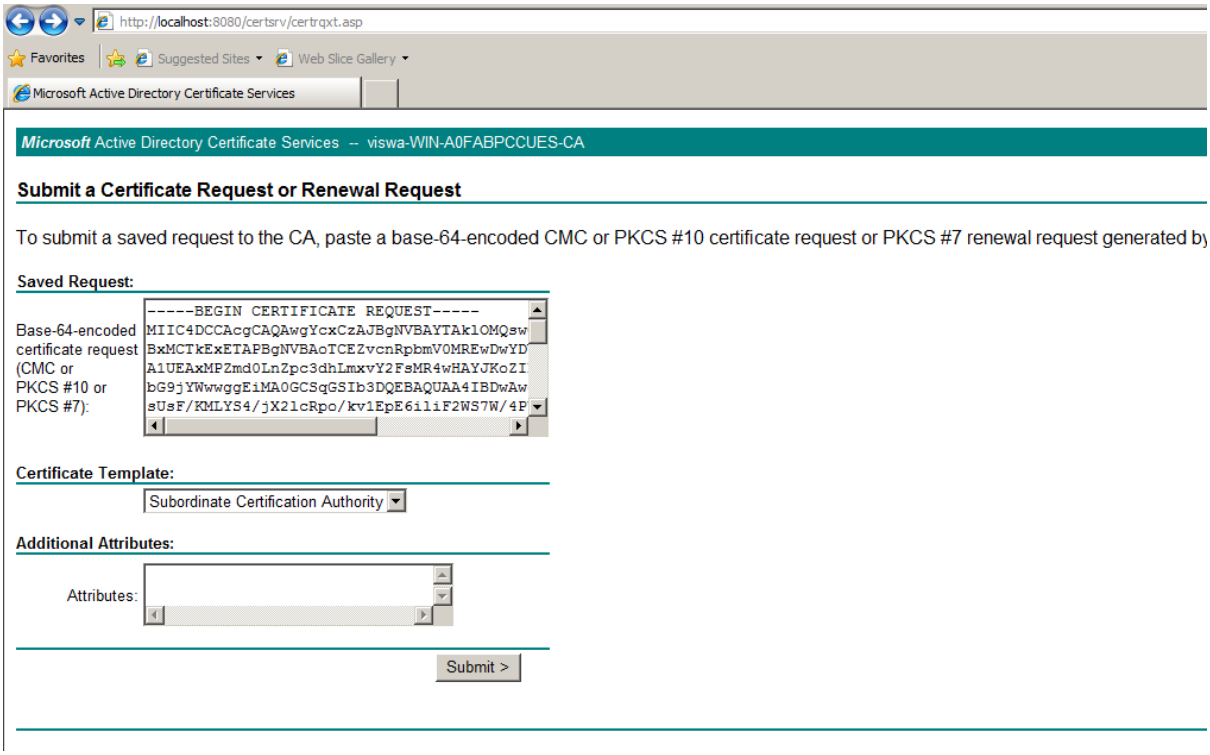


- Go to System >> Certificates >> Local Certificates >> Select certificate created in the previous step and click on Download button to download the CSR.

Step2

➢ Sign the CSR on Windows CA and download the signed certificate from Windows CA.

- Go to Active directory Web enrolment page on your Windows CA.
- Click on “Request a certificate”
- Select “Advanced certificate request”
- Select “Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file”
- Using text editor (notepad), open the CSR downloaded in step1.
- Copy the contents of the CSR to clipboard and paste the contents of the certificate in “Saved Request”
- In “Certificate Template”, select template as “Subordinate Certifcate Authority” and Click “Submit” button.

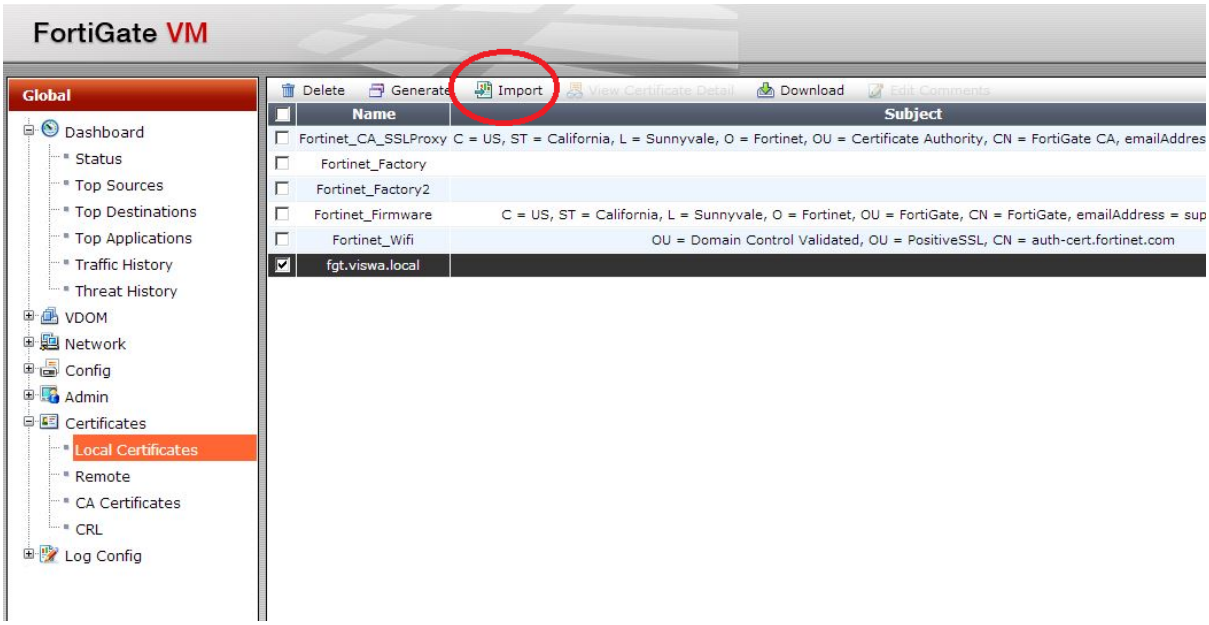


- Download the certificate in next screen and save it locally on hard drive.

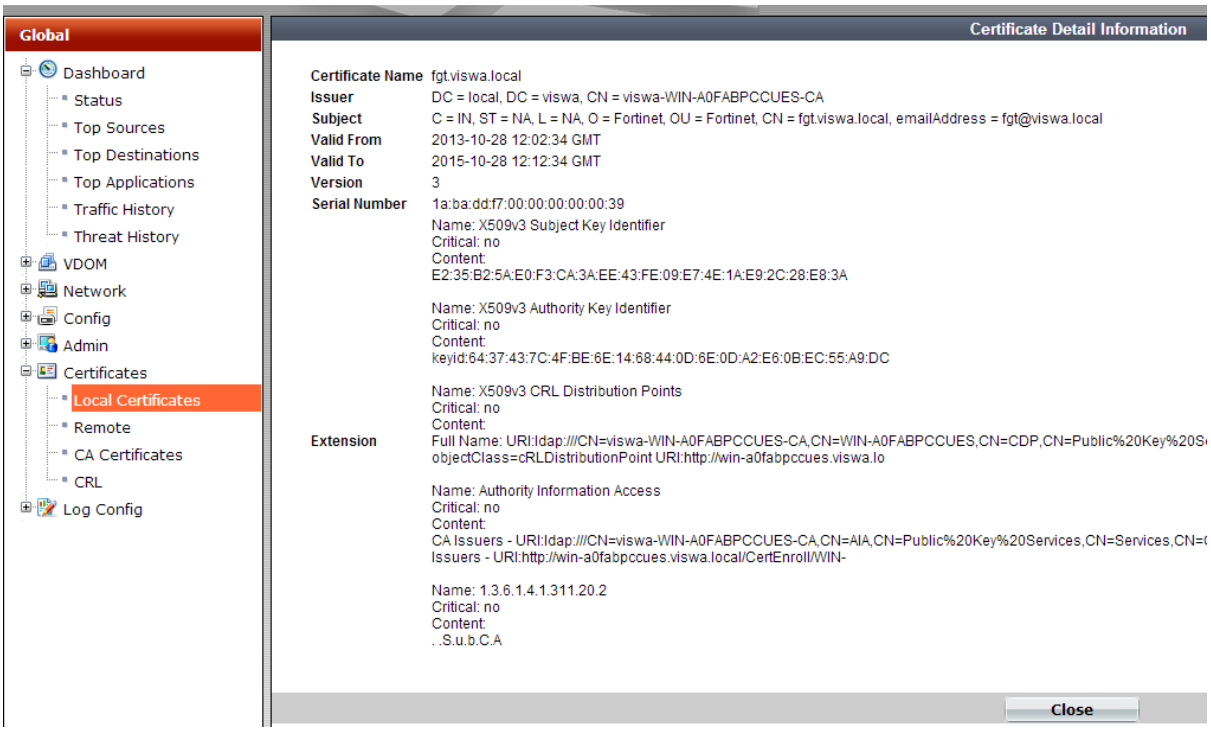
Step3

➢ Import the signed certificate on to FortiGate unit.

- Log in to FortiGate unit GUI >> Go to System >> Certificates >> Local Certificates >> Select the certificate signing request created in step1 and click on “Import” button.



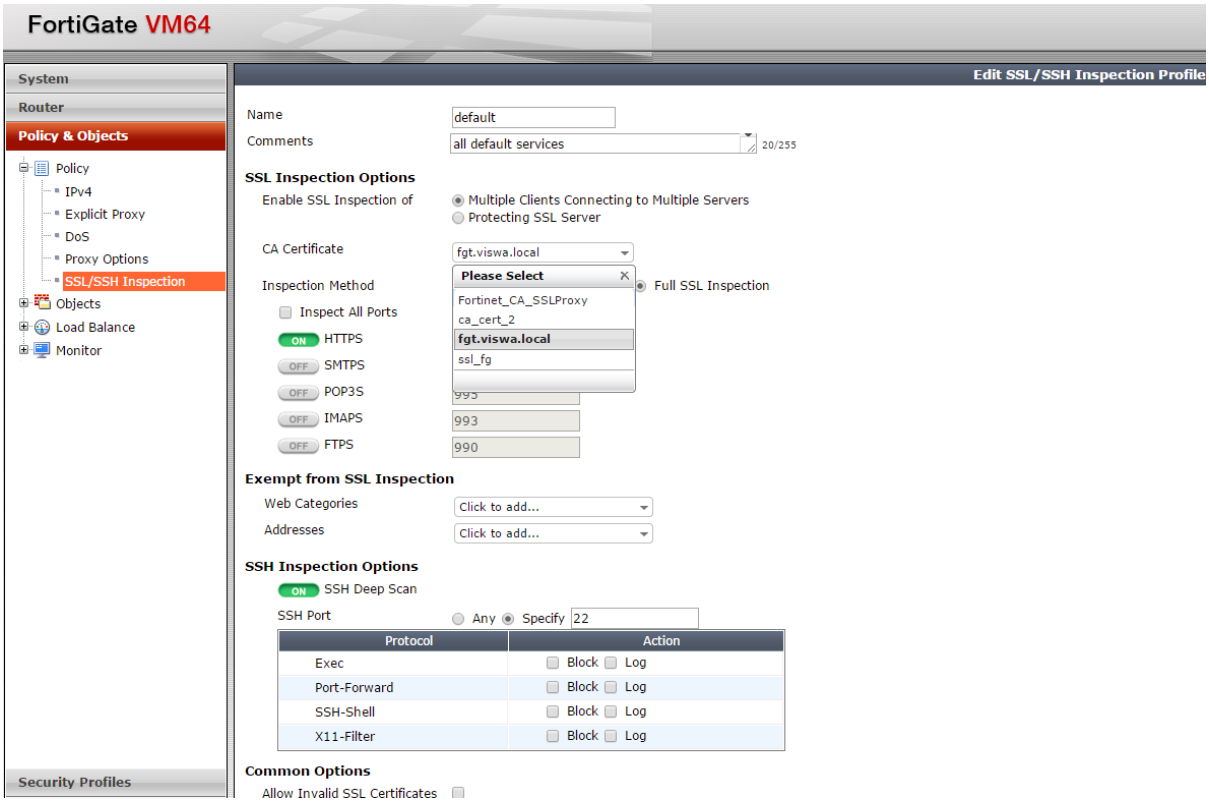
- In the Import certificate page, select Type as “Certificate” and Click on Choose file Button.
- Navigate to the Certificate downloaded from Windows CA in step 2, select the certificate and click on OK. You will get message “Upload Certificate successfully”
- Click on Return button and verify the certificate has been imported properly.



Step4

- Configure SSL inspection to use the new certificate.

You can select the SSL inspection certificate under: Policy >> Policy >> SSL/SSH Inspection Options >> Select the profile used in firewall policy >> CA Certificate



Step5

- Verification.

Since the SSL inspection certificate is signed by the domain controller CA, all the hosts part of the domain will trust the CA certificate. When client access a HTTPS website with deep scan/SSL full inspection enabled on FortiGate unit, browser will not display certificate error message.